of work to compute and work to invert. This class of functions, however, is not required to be completely intractable, but alternatively should have some measurable difference in the amount of work required to invert, compared to the cost of calculation of the output of the function. The application of this invention to key escrowing is described. A basic algorithm for implementation as an example of a suitable limited one-way function is described. This problem involves randomization and can be viewed as an extension of the puzzling problem originally developed by Ralph C. Merkle, "Secure Communications Over Insecure Channels," Communications of the ACM, April 1978, Volume 21, Number 4, pages 294-299. The basic algorithm utilized in implementation of the invention requires a randomized response and achieves a limited, but measurable computational advantage of the data receiver over an eavesdropper. Algorithm performance and application to the implementation of a delay function for employment in key escrow systems is hereinafter explained.

a1

IN THE CLAIMS:

For the convenience of the Examiner, all pending claims are shown below whether or not an amendment has been made.

1. (Amended) Apparatus for multiplication of modular numbers, comprising:

a two-dimensional dependency array of selectively coupled cells, where each cell comprises:

a first full adder receiving a first input signal, a second input signal, and a clock signal,

a second full adder receiving an output of the first full adder, a third input signal, and a clock signal;

a2

a half adder receiving an output of the second full adder and a fourth input signal;

a first storage circuit coupled to the second full adder;

a second storage circuit coupled to the half adder; and

a third storage circuit coupled to the half adder.